EC-Council

Exam Questions 212-81

EC-Council Certified Encryption Specialist (ECES)

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
Which of the following is a type of encryption that has two different keys. One key can encrypt the message and the other key can only decrypt it?

A. Block cipher
B. Asymmetric
C. Symmetric
D. Stream cipher

Answer: B

NEW QUESTION 2
If you wished to see a list of revoked certificates from a CA, where would you look?

A. RA
B. RFC
C. CRL
D. CA

Answer: C

NEW QUESTION 3
Which one of the following terms describes two numbers that have no common factors?

A. Coprime
B. Fermat's number
C. Euler's totient
D. Convergent

Answer: A

NEW QUESTION 4
What is the largest key size that AES can use?

A. 256
B. 56
C. 512
D. 128

Answer: A

NEW QUESTION 5
A digital document that contains a public key and some information to allow your system to verify where that key came from. Used for web servers, Cisco Secure phones, E- Commerce.

A. Registration Authority
B. Payload
C. OCSP
D. Digital Certificate

Answer: D

NEW QUESTION 6
What is the name of the attack where the attacker obtains the ciphertexts corresponding to a set of plaintexts of his own choosing?

A. Chosen plaintext
B. Differential cryptanalysis
C. Known-plaintext attack
D. Kasiski examination

Answer: A

NEW QUESTION 7
With Electronic codebook (ECB) what happens:

A. The message is divided into blocks and each block is encrypted separatel
B. This is the most basic mode for symmetric encryption
C. The cipher text from the current round is XORed with the plaintext from the previous round
D. The block cipher is turned into a stream cipher
E. The cipher text from the current round is XORed with the plaintext for the next round

Answer: A

NEW QUESTION 8

Which of the following is a fundamental principle of cryptography that holds that the algorithm can be publicly disclosed without damaging security?

A. Vigenere's principle
B. Shamir's principle
C. Kerkchoff's principle
D. Babbage's principle

Answer: C

NEW QUESTION 9
Original, unencrypted information is referred to as _____.

A. text
B. plaintext
C. ciphertext
D. cleartext

Answer: B

NEW QUESTION 10
Protocol suite provides a method of setting up a secure channel for protected data exchange between two devices.

A. CLR
B. OCSP
C. TLS
D. IPSec

Answer: D

NEW QUESTION 10
What is the formula m^e %n related to?

A. Encrypting with EC
B. Decrypting with RSA
C. Generating Mersenne primes
D. Encrypting with RSA

Answer: D

NEW QUESTION 13
A transposition cipher invented 1918 by Fritz Nebel, used a 36 letter alphabet and a modified Polybius square with a single columnar transposition.

A. ADFVGX Cipher
B. ROT13 Cipher
C. Book Ciphers
D. Cipher Disk

Answer: A

NEW QUESTION 16
Which of the following is an asymmetric algorithm that was first publically described in 1977?

A. Elliptic Curve
B. Twofish
C. DESX
D. RSA

Answer: D

NEW QUESTION 21
When learning algorithms, such as RSA, it is important to understand the mathematics being used. In RSA, the number of positive integers less than or equal to some number is critical in key generation. The number of positive integers less than or equal to n that are coprime to n is called _____.

A. Mersenne's number
B. Fermat's number
C. Euler's totient
D. Fermat's prime

Answer: C

NEW QUESTION 22
If the round function is a cryptographically secure pseudorandom function, then _____ rounds is sufficient to make it a "strong" pseudorandom permutation.

A. 15
B. 16

C. 3
D. 4

Answer: D

NEW QUESTION 23
A measure of the uncertainty associated with a random variable.

A. Collision
B. Whitening
C. Diffusion
D. Entropy

Answer: D

NEW QUESTION 28
Early attempt to make substitution ciphers more robust, masks letter frequencies, plain text letters map to multiple cipher text symbols.

A. Scytale Cipher
B. Playfair Cipher
C. Homophonic Substitution
D. ADFVGX Cipher

Answer: C

NEW QUESTION 32
Which of the following are valid key sizes for AES (choose three)?

A. 192
B. 56
C. 256
D. 128
E. 512
F. 64

Answer: ACD

NEW QUESTION 36
Why is quantum computing a threat to RSA?

A. The processing speed will brute force algorithms
B. Quantum computers can solve the discrete logarithm problem
C. Quantum computers can solve the birthday paradox
D. Quantum computers can factor large integers in polynomial time

Answer: D

NEW QUESTION 38
Which of the following is an asymmetric cipher?

A. RSA
B. AES
C. DES
D. RC4

Answer: A

NEW QUESTION 40
Which of the following is a block cipher?

A. AES
B. DH
C. RC4
D. RSA

Answer: A

NEW QUESTION 45
You are explaining the details of the AES algorithm to cryptography students. You are discussing the derivation of the round keys from the shared symmetric key. The portion of AES where round keys are derived from the cipher key using Rijndael's key schedule is called what?

A. The key expansion phase
B. The round key phase
C. The bit shifting phase
D. The initial round

Answer: A

NEW QUESTION 49
Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?

A. IPsec Policy Agent
B. Internet Key Exchange (IKE)
C. Oakley
D. IPsec driver

Answer: B

NEW QUESTION 54
If Bob is using asymmetric cryptography and wants to send a message to Alice so that only she can decrypt it, what key should he use to encrypt the message?

A. Alice's private key
B. Bob's private key
C. Alice's public key
D. Bob's public key

Answer: C

NEW QUESTION 58
Message hidden in unrelated text. Sender and receiver have pre-arranged to use a pattern to remove certain letters from the message which leaves only the true message behind.

A. Caesar Cipher
B. Null Ciphers
C. Vigenere Cipher
D. Playfair Cipher

Answer: B

NEW QUESTION 59
Algorithm that was chosen for the Data Encryption Standard, which was altered and renamed Data Encryption Algorithm.

A. Blowfish
B. Rijndael
C. Lucifer
D. El Gamal

Answer: C

NEW QUESTION 64
John is trying to select the appropriate authentication protocol for his company. Which of the following types of authentication solutions use tickets to provide access to various resources from a central location?

A. Kerberos
B. EAP
C. Radius
D. CHAP

Answer: A

NEW QUESTION 68
Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

A. Key distribution
B. Security
C. Scalability
D. Speed

Answer: D

NEW QUESTION 69
A disk you rotated to encrypt/decrypt. Created by Leon Alberti. Similar technologies were used in the Enigma machine. Considered the forefather of modern encryption.

A. Chi Square
B. Enigma Machine
C. Cipher Disks
D. Scytale Cipher

Answer: C

NEW QUESTION 70
Symmetric algorithm. Designed by James Massey and Xuejia Lai. Operates on 64 bit blocks and has a 128 bit key. Consists of 8 identical transformations each round and an output transformation.

A. IDEA
B. RSA
C. CAST
D. DES

Answer: A

NEW QUESTION 71
Numbers that have no factors in common with another.

A. Fibonacci Numbers
B. Even Numbers
C. Co-prime numbers
D. Mersenne Primes

Answer: C

NEW QUESTION 75
Which of the following asymmetric algorithms is described by U.S. Patent 5,231,668 and FIPS 186

A. AES
B. RC4
C. DSA
D. RSA

Answer: C

NEW QUESTION 78
Which of the following is generally true about key sizes?

A. Larger key sizes increase security
B. Key size is irrelevant to security
C. Key sizes must be more than 256 bits to be secure
D. Smaller key sizes increase security

Answer: A

NEW QUESTION 81
The most widely used asymmetric encryption algorithm is what?

A. Vigenere
B. Caesar Cipher
C. RSA
D. DES

Answer: C

NEW QUESTION 82
A _____ product refers to an NSA-endorsed classified or controlled cryptographic item for classified or sensitive U. S. government information, including cryptographic equipment, assembly, or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed

A. 1
B. 4
C. 2
D. 3

Answer: A

NEW QUESTION 85
In relationship to hashing, the term _____ refers to random bits that are used as one of the inputs to the hash. Essentially the _____ is intermixed with the message that is to be hashed

A. Vector
B. Salt
C. Stream
D. IV

Answer: B

NEW QUESTION 88

The most widely used digital certificate standard. First issued July 3, 1988. It is a digital document that contains a public key signed by the trusted third party, which is known as a Certificate Authority, or CA. Relied on by S/MIME. Contains your name, info about you, and a signature of a person who issued the certificate.

A. ElGamal
B. RSA
C. PAP
D. X.509

Answer: D

NEW QUESTION 93
Changing some part of the plain text for some matching part of cipher text. Historical algorithms typically use this.

A. Decoding
B. Substitution
C. Transposition
D. Collision

Answer: B

NEW QUESTION 95
Ciphers that write message letters out diagonally over a number of rows then read off cipher row by row. Also called zig-zag cipher.

A. Rail Fence Cipher
B. Null Cipher
C. Vigenere Cipher
D. ROT-13

Answer: A

NEW QUESTION 96
A cryptanalysis success where the attacker deduces the secret key.

A. Information Deduction
B. Avalanche effect
C. Shannon's Entropy
D. Total Break

Answer: D

NEW QUESTION 101
A number that is used only one time, then discarded is called what?

A. IV
B. Nonce
C. Chain
D. Salt

Answer: B

NEW QUESTION 106
Which algorithm implements an unbalanced Feistel cipher?

A. Skipjack
B. RSA
C. 3DES
D. Blowfish

Answer: A

NEW QUESTION 110
Calculates the average LSB and builds a table of frequencies and Pair of Values. Performs a test on the two tables. It measures the theoretical vs. calculated population difference.

A. Certificate Authority
B. Raw Quick Pair
C. Chi-Square Analysis
D. SP network

Answer: C

NEW QUESTION 113
The time and effort required to break a security measure.

A. Session Key

B. Work factor
C. Non-repudiation
D. Payload

Answer: B

NEW QUESTION 118
Which one of the following best describes a process that splits the block of plaintext into two separate blocks, then applies the round function to one half, and finally swaps the two halves?

A. Block ciphers
B. Symmetric cryptography
C. Feistel cipher
D. Substitution cipher

Answer: C

NEW QUESTION 122
What is the basis for the difficulty in breaking RSA?

A. Hashing
B. The birthday paradox
C. Equations that describe an elliptic curve
D. Factoring numbers

Answer: D

NEW QUESTION 127
How can rainbow tables be defeated?

A. Lockout accounts under brute force password cracking attempts
B. All uppercase character passwords
C. Use of non-dictionary words
D. Password salting

Answer: D

NEW QUESTION 131
A linear congruential generator is an example of what?

A. A coprime generator
B. A prime number generator
C. A pseudo random number generator
D. A random number generator

Answer: C

NEW QUESTION 134
Which of the following would be the weakest encryption algorithm?

A. DES
B. AES
C. RSA
D. EC

Answer: A

NEW QUESTION 138
An authentication method that periodically re-authenticates the client by establishing a hash that is then resent from the client is called _____ .

A. CHAP
B. SPAP
C. PAP
D. EAP

Answer: A

NEW QUESTION 141
A simple algorithm that will take the initial key and from that generate a slightly different key each round.

A. Key Schedule
B. Feistel Network
C. SHA-2
D. Diffie-Helman

Answer: A

NEW QUESTION 143
Storing private keys with a third party is referred to as what?

A. Key caching
B. Key storage
C. Key banking
D. Key escrow

Answer: D

NEW QUESTION 148
Electromechanical rotor-based cipher used in World War II

A. ROT13 Cipher
B. Cipher Disk
C. Enigma Machine
D. Rail Fence Cipher

Answer: C

NEW QUESTION 150
_____ cryptography uses one key to encrypt a message and a different key to decrypt it.

A. Secure
B. Asymmetric
C. Stream
D. Symmetric

Answer: B

NEW QUESTION 151
.....

Relate Links

100% Pass Your 212-81 Exam with Exambible Prep Materials

https://www.exambible.com/212-81-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/